Managed Embedded Security Controls Service
Annex to the BT Managed Service Schedule

Contents

Managed Embedded Security Controls Service Annex

Application of this Annex

This Annex sets out the additional terms that will apply where BT provides you with the Managed Embedded Security Controls Service. The terms of this Annex apply in addition to the terms set out in:

(a) the Schedule; and
(b) the General Terms.

A note on 'you'

'You' and 'your' mean the Customer.

Words defined in the General Terms

Words that are capitalised but have not been defined in this Annex have the meanings given to them in the General Terms or the Schedule.

Part A – The Managed Embedded Security Controls Service

1 Service Summary

BT will provide you with a right to access Embedded Security Controls enabling you to protect your Users from threats from the Internet, comprising:

1.2 the Standard Service Components; and

1.3 any of the Service Options as set out in Paragraph 3 that are selected by you as set out in any applicable Order,

up to the point of the Service Management Boundary as set out in Paragraph 4 ("**Managed Embedded Security Controls Service**").

2 Standard Service Components

BT will provide you with all the following standard service components ("**Standard Service Components**") in accordance with the details as set out in any applicable Order:

2.1 **Aggregated Bandwidth Consumption**

2.1.1 BT will provide you with the availability of the following range of aggregated bandwidth consumptions to access the Internet required by you:

(a) <100Mb;
(b) 100Mb – 500Mb;
(c) 500Mb – 1Gb;
(d) 1Gb – 5Gb; or
(e) 5Gb – 10Gb.

2.1.2 BT may monitor the aggregated Internet traffic bandwidth consumption used by you in accordance with the consumption purchased. BT may require you to purchase more aggregated bandwidth at an additional Charge where you go over your aggregated bandwidth consumption purchased. BT may not be able to provide you with the full Managed Embedded Security Controls Service if you do not purchase more aggregated bandwidth as required by BT.

2.2 **Security Event Reporting**:

2.2.1 BT will provide reporting facilities on-line which allows analysis of security-related events.

2.2.2 BT will not pro-actively view your reports and events for security incidents as part of this Standard Service Component.

2.2.3 If this Standard Service Component is delivered via a shared reporting platform, BT will configure the platform such that you are only provided with access to your reports. This may mean that some of the platform's functionality is restricted to preserve the confidentiality of all customers using that platform.

2.2.4 The period over which data can be analysed is dependent on the capacity of the Security Appliances or the space allocated on the reporting platform.

2.2.5 If you select the SSL/TLS Inspection Service Option set out in Paragraph 3.7, BT will be able to scan SSL Encrypted Traffic in the same way that non-encrypted traffic can be scanned, provided your CSP permits such scanning.

2.3 **High Availability (dual appliance) solutions:**

2.3.1 BT will configure the Managed Embedded Security Controls Service to provide resilience against multiple failures, utilising both hardware resilience with the Embedded Security Controls network nodes and failover between Embedded Security Controls network nodes to ensure high availability of the Managed Embedded Security Controls Service.

2.4 **Initial Setup**

BT will as part of the initial setup:

2.4.1 commission the Embedded Security Controls and establish a remote link from your networked Customer Equipment to the Embedded Security Controls; and

2.4.2 monitor and manage the Embedded Security Controls in accordance with this Annex and the Schedule.

3 Service Options

BT will provide you with any of the following options ("**Service Options**") as set out in any applicable Order and in accordance with the details as set out in that Order.

3.1 **URL Filtering and Application Control**

3.1.1 BT will:

(a) block access to the Internet sites that you ask BT to, in accordance with your CSP;

(b) send an appropriate message to a User attempting to access a blocked or restricted Internet site to advise either;

(i) that the User request has been blocked; or

(ii) that the User will first confirm acceptance of your acceptable use policy (or similar warning) and upon acceptance by the User, the page will be delivered; and

(c) implement any alterations, via the standard configuration management process, in the event of any change in your CSP.

3.2 **Anti-Virus**

3.2.1 BT will:

(a) check web browser (http) traffic for known malware;

(b) inspect requests from Users for an executable file from a site on the Internet, against the current antivirus definition file set out in the applicable intrusion signature files. If no virus is detected, the file will be passed to the User. If a virus is detected the file will be blocked and deleted; and

(c) keep antivirus definition files up to date by regular downloads direct from the firewall supplier.

3.3 **Anti-Bot**

3.3.1 BT will check and block outbound traffic for communication with known command and control servers used by owners of malicious software.

3.4 **VPNs**

3.4.1 BT will set up and configure the following types of VPN in accordance with BT's prevailing technical standards:

(a) remote access IPSec/SSL VPNs, for remote Users to gain secure access to your internal network. BT will implement your rules to authenticate against your authentication server. You are responsible for providing and installing your own end-user VPN software; and

(b) Site to Site IPSec VPNs between two Security Appliances managed by BT.

3.4.2 Where a digital certificate is required for remote VPN set up, either BT will provide, or you will provide to BT, as set out in the Order, an up-to-date digital certificate that will be installed on the Security Appliance.

3.4.3 Where you provide the digital certificate, BT will install it within seven days of receipt from you.

3.4.4 If you have selected Managed Service Package 3, BT will notify you of the date of expiry of the digital certificate three months prior to the date of expiry. You will advise BT, in writing, within one month of the date of BT's notification whether or not you want to renew your digital certificate.

3.4.5 If you want to renew your digital certificate and it is your responsibility as set out in the Order to provide BT with the digital certificate, you will provide the new digital certificate to BT at least seven days prior to the expiry of the original digital certificate.

3.4.6 BT will not be liable for issues caused by expired digital certificates if:

(a) you do not confirm to BT that you want to renew your digital certificate in accordance with Paragraph 3.4.4; or

(b) you do not provide BT with an up-to-date digital certificate in accordance with Paragraph 3.4.5.

3.5 **Intrusion Detection and Prevention Service ("IPS")**

3.5.1 BT will:

(a) monitor traffic passing through your Security Appliance for attacks, in accordance with the applicable intrusion signature files; and

(b) implement IPS with a default configuration setting, as defined by BT. BT will also maintain a subscription to the necessary signature updates, and arrange for these to be applied following issue by the supplier.

3.5.2 BT will not be responsible for evaluating these signatures beforehand.

3.5.3 BT will advise you how the IPS that you have selected operates with regard to alerting or IPS specific reporting.

3.5.4 If BT agrees a request from you to alter the parameters for applying new signatures in "**block**" mode to give a greater or lower sensitivity to attacks, you accept responsibility for the increased risk of false positives (blocks to legitimate traffic) or the increased risk of attacks being missed.

3.5.5 If you select the SSL/TLS Inspection Service Option set out in Paragraph 3.7, BT will be able to scan SSL Encrypted Traffic in the same way that non-encrypted traffic can be scanned, provided your CSP permits such scanning.

3.6 **Threat Emulation Service**

3.6.1 The Threat Emulation Service will only be available if you have selected the Managed Service Package 3 under the Schedule.

3.6.2 BT will encrypt suspected malicious files and send them to the vendor's cloud-based infrastructure where they will be decrypted and analysed for malware by reviewing its behaviour in a virtual environment (sandbox).

3.6.3 You may be able to choose whether to hold the file whilst it is being analysed (to provide increased security) or to release it and analyse it in the background (for improved User response). Background processing may lead to malicious files being permitted until signature updates are subsequently generated and applied to your Security Appliances.

3.6.4 If a file has been deemed malicious, its characteristics will be added to the vendor's anti-virus signature list.

3.6.5 BT will determine the country in which this inspection and analysis occurs.

3.6.6 If the SSL/TLS Inspection Service Option set out in Paragraph 3.7 is selected, BT will be able to scan SSL Encrypted Traffic in the same way that non-encrypted traffic can be scanned, provided your CSP permits such scanning.

3.6.7 Submission and processing of your data via the Threat Emulation Service will be at your sole discretion and at your own risk. Other than BT's obligations in Clause 14 of the General Terms, BT assumes no responsibility or liability for the receipt and processing of such data.

3.7 **SSL/TLS Inspection**

3.7.1 BT will intercept and decrypt SSL Encrypted Traffic in order to carry out inspection in accordance with the CSP. Once the traffic has been inspected, it will be re-encrypted and relayed to its original destination (if permitted by the CSP).

3.7.2 BT will not intercept and decrypt SSL Encrypted Traffic for every category of web content due to a high possibility of issues with associated applications with certain websites e.g. some websites may not permit decryption.

3.7.3 The provisions set out in Paragraphs 3.4.2 to 3.4.6, in relation to digital certificates apply to SSL/TLS Inspection.

3.8 **Identity Awareness/User Groups:**

3.8.1 The Identity Awareness/User Groups Service Option will only be available if you have selected the Managed Service Package 3 under the Schedule.

3.8.2 BT will configure the features of the Security Appliance that support the Identity Awareness/User Groups to apply certain rules of the CSP according to the authenticated identity of the User rather than just their IP Address.

3.8.3 This may require Software to be installed within your network or on end-user devices, or ensuring BT has remote, read-only, access to your active directory authentication server.

3.8.4 You will maintain the authentication database of Users, groups and any access credentials that you require.

4 Service Management Boundary

4.1 BT will provide and manage the Managed Embedded Security Controls Service as set out in Parts A, B and C of this Annex and as set out in the Order. The service management boundary is the point where traffic enters and leaves the infrastructure owned or controlled by BT ("**Service Management Boundary**").

4.2 BT will have no responsibility for the Managed Embedded Security Controls Service outside the Service Management Boundary including:

4.2.1 issues on User machines (e.g. operating system, coding languages and security settings);

4.2.2 end to end network connectivity (e.g. your network or networking equipment, Internet connectivity), unless agreed with BT;

4.2.3 identity source management;

4.2.4 policy ownership; or

4.2.5 security information and event management analysis.

4.3 BT does not guarantee that the Managed Embedded Security Controls Service will detect or block all malicious threats.

4.4 BT does not make any representations, whether express or implied, about whether the Managed Embedded Security Controls Service will operate in combination with any Customer Equipment or other equipment and software, unless agreed with BT.

5 Associated Services and Third Parties

5.1 You will provide and maintain an Internet connection at the Site(s) at all times for use with the Managed Embedded Security Controls Service, including providing and maintaining any Customer Equipment necessary for such connection. You will pay all charges related to provision, maintenance and use of such Internet connections and report any incidents on the Internet connections directly to the supplier of the compatible Internet connections.

5.2 If BT provides you with any additional services this Annex will not apply to those services and those services will be governed by their separate terms.

5.3 BT will not be liable for failure to or delay in supplying the Managed Embedded Security Controls Service if another supplier delays or refuses the supply of an electronic communications service to BT and no alternative service is available at reasonable cost.

6 Specific Terms

6.1 **Customer Committed Date**

6.1.1 If you request a change to the Managed Embedded Security Controls Service or any part of the Managed Embedded Security Controls Service, then BT may revise the Customer Committed Date to accommodate that change.

6.1.2 BT may expedite delivery of the Managed Embedded Security Controls Service for operational reasons or in response to a request from you, but this will not revise the Customer Committed Date.

6.2 **Service Amendment**

In addition to what is set out in Clause 31 of the General Terms:

6.2.1 throughout the Minimum Period of Service, you may request an increase or decrease of the aggregated bandwidth consumption supplied, subject to capacity and the current bandwidth consumption by you;

6.2.2 any bandwidth increase or decrease will be chargeable by BT and will operate for a minimum period of five Business Days before you may make any further requests; and

6.2.3 where a bandwidth increase is beyond the available capacity of your current Managed Embedded Security Controls Service, BT will ensure your IPSec tunnels are re-routed via a different IP Address. BT may require you to change your IP Address.

6.3 **Licence**

6.3.1 BT gives you a non-exclusive, non-transferable and limited right to use the Managed Embedded Security Controls Service for your internal business purposes only.

6.3.2 You will not resell or otherwise transfer the Managed Embedded Security Controls Service or other licences granted under this Contract.

6.4 **Invoicing**

6.4.1 BT may invoice you for any of the following Charges in addition to those set out in the Schedule or any applicable Order:

(a) an increase or decrease of the aggregated bandwidth consumption in accordance with Paragraphs 2.1.2 and 6.2 of this Annex; and

(b) Charges for expediting provision of the Managed Embedded Security Controls Service at your request after BT has informed you of the Customer Committed Date.

6.5 **Amendments to the Managed Service Schedule**

6.5.1 Paragraphs 2.5, 2.6, 2.7, 2.8 and 2.9 of the Schedule will not apply.

6.5.2 The wording in Paragraph 2.10 of the Schedule is deleted and replaced with the following:

2.10 **Software Upgrades**

2.10.1 BT will apply remotely Software upgrades at its convenience.

2.10.2 Remotely updating Software does carry some risk of the Managed Embedded Security Controls Service not returning to an operational state immediately and BT may require you to test the Managed Embedded Security Controls Service to check it is operating as expected.

2.10.3 BT will notify you as soon as reasonably practicable of the duration and impact of Managed Embedded Security Controls Service downtime as a result of BT installing the Software updates.

6.5.3 The wording in Paragraphs 2.11 of the Schedule is deleted and replaced with the following:

2.11 **Performance Reporting**

2.11.1 Not used.

2.11.2 **Service Reporting**

BT will deliver to you, on a monthly basis, a Service Report showing the number of Incidents reported and resolved in relation to your Associated Services ("Service Reporting").

2.11.3 Not used.

2.11.4 Not used.

2.11.5 Not used.

2.11.6 **Vendor Network and Application Reporting**

BT will provide you with access to the Managed Services Portal where you can access performance reports on your Associated Services ("**Vendor Network and Application Reporting**").

6.5.4 Paragraphs 2.12 and 2.13 of the Schedule will not apply.

6.5.5 The wording in Paragraphs 2.14 and 2.15 of the Schedule is deleted and replaced with the following:

2.14 **Change Management – Simple Service Requests**

2.14.1 BT will provide you with a simple service request service ("SSR") that enables you to request changes to your Managed Service and Associated Services.

2.14.2 BT will only proceed with a SSR once you have provided BT with all information that BT reasonably requires to complete the SSR.

2.14.3 BT will provide you with access to the Managed Services Portal that will allow you to request, manage and monitor the progress of your SSRs.

2.14.4 BT will assign each SSR a value in unit credits. The more complex or time consuming an SSR is to implement, then the more unit credits will be associated with the SSR.

2.14.5 You may only have 40 live separate SSRs requests open at any one time across all your Associated Services.

2.14.6 BT will apply Standard Delivery Lead Times to a maximum of four SSRs and agree specific delivery lead-times with you for five or more SSRs.

2.14.7 You may buy additional credits for SSRs at any time for an additional Charge.

2.14.8 If you choose the Managed Service 1 Package, BT will provide you with SSR Pay as You Go through which:

(a) you will be able to buy a pre-paid bundle of SSRs and use this bundle to pay for any SSRs you submit through the Managed Services Portal ("SSR Pay as You Go");

2.14.9 Where you have purchased pre-paid bundles:

(a) you may top up or buy additional SSRs when you have consumed your pre-paid bundle of SSRs;

(b) BT will not refund any Charges for unused SSR credit units; and

(c) if you have a negative balance of credit units outstanding for two consecutive weeks, BT will charge you for these credit units on your next invoice.

2.14.10 If you choose the Managed Service 2 Package, BT will allocate you five SSRs per annum per Site ("SSR 5").

2.14.11 If you choose the Managed Service 3 Package or Managed Service Cloud Package, BT will allocate you 10 SSRs per annum per Site ("SSR 10").

2.15 In respect of any changes to your Associated Services:

2.15.1 BT will implement the SSRs by means of a management link between your Host Site and BT's management centre;

2.15.2 you will pay BT Charges for the work involved in reviewing existing configurations and any subsequent work; and

2.15.3 you will provide BT an up-to-date inventory of MS Equipment to be covered by any requested SSRs and BT can do so on your behalf in respect of certain Associated Services for an additional Charge.

6.5.6 The wording in Paragraph 2.16 of the Schedule is deleted and replaced with the following:

2.16 **Packaged Deployment Services**

2.16.1 **PDS Project Management**

BT will provide you with an implementation service covering project management, coordination, detailed solution design, installation, configuration, commissioning, acceptance testing and rollout of the Associated Services at your Site ("**PDS Project Management**").

2.16.2 **PDS Project Coordination**

(a) BT will appoint a project coordinator who will co-ordinate the implementation of the Associated Service and act as a single point of contact for you in all matters relating to the project ("**Project Coordinator**").

(b) The Project Coordinator will be office based and will not conduct face to face meetings with you.

2.16.3 **PDS Hybrid Project Management**

(a) BT will appoint a BT project manager who will act as a single point of contact in respect of the management, detailed solution design, installation, configuration, commissioning, acceptance testing and roll-out of the Associated Service ("**BT Project Manager**").

(b) The BT Project Manager will be available to meet with you up to three times which will take the form of:

(i) an initial meeting to agree the implementation plan for your Associated Service;

(ii) a meeting at an agreed midpoint in the delivery of your Associated Service; and

(iii) a project review meeting towards the conclusion of the delivery of your Associated Services.

(c) You will be charged for the PDS Hybrid Project Management service on a full day rate basis only and not on a partial or across day basis.

(d) For an additional Charge and on reasonable notice, you may order up to two additional PDS Hybrid Project Management face to face day visits.

(e) You will be charged for all reasonable travel and accommodation expenses if you require the BT Project Manager to travel outside the UK.

2.16.4 **PDS Face to Face Project Management**

(a) BT will appoint a BT Project Manager to manage the implementation of your Associated Service and will act as a single point of contact for you in all matters relating to the installation of your Associated Service.

(b) The BT Project Manager will be available to meet you face to face on a reasonable number of occasions as agreed between the both of us to agree the implementation plan and conduct project review meetings as appropriate.

(c) You will be charged for all reasonable travel and accommodation expenses if you require the BT Project Manager to travel outside the UK.

2.16.5 Not used.

2.16.6 Not used.

2.16.7 Not used.

2.16.8 **PDS Installation Services**

(a) BT will provide you with a managed installation service for your Associated Services consisting of the delivery, unpacking and installation of any MS Equipment to your Site ("**PDS Installation Services**").

(b) BT will require access to your Site during Business Hours but may, on reasonable notice, require you to provide access at other times.

(c) Any MS Equipment will be supplied with the manufacturer's standard software configuration.

(d) Not used.

(e) BT will prepare a configuration based on the contracted design and configuration information that you provide BT with. You will pay additional Charges for any subsequent request for additional work outside the scope of the original configuration.

(f) On BT`s request, you will provide BT with all configuration information, so that BT can provide an operational configuration. You will submit the specified configuration information to BT in the form of a completed Customer requirement document.

(g) BT is not responsible for any work or testing on any form of network, other than to demonstrate that the configuration is working correctly.

6.5.7 Regardless of what it may say in Paragraph 4.2 of the Schedule:

(a) at the end of the Minimum Period of Service, unless one of us has given Notice to the other of an intention to terminate the Managed Embedded Security Controls Service in accordance with the Contract, BT will continue to provide the Managed Embedded Security Controls Service and each of us will continue to perform our obligations in accordance with the Contract;

(b) if the Managed Embedded Security Controls Service is the only Associated Service purchased under the Contract for the Managed Service, Paragraph 4.2 of the Schedule will not apply to the Managed Service and Paragraph 6.5.7 of this Annex will apply; and

(c) if the Managed Embedded Security Controls Service is purchased along with other Associated Services under the Contract for the Managed Service, Paragraph 4.2 of the Schedule will apply to the Managed Service and the other Associated Services and Paragraph 6.5.7(a) of this Annex will apply only to the Managed Embedded Security Controls Service.

6.5.8 Regardless of what it may say in Paragraphs 4.3.2 and 4.3.3 of the Schedule, if either of us terminates the Managed Service in accordance with Paragraph 4.3.1 of the Schedule, the Managed Embedded Security Controls Service will automatically terminate at the same time and you will pay Termination Charges in accordance with Paragraph 4.7 of the Schedule as amended by this Annex.

6.5.9 The wording in Paragraph 4.7.2 of the Schedule is deleted and replaced with the following:

4.7.2 In addition to the Charges set out at Paragraph 4.7.1 above, if you terminate the Managed Embedded Security Controls Service during the Minimum Period of Service you will pay BT:

(a) for any parts of the Managed Embedded Security Controls Service that were terminated during the first 12 months of the Minimum Period of Service, Termination Charges, as compensation, equal to 100 per cent of the Recurring Charges for any remaining months of the first 12 months of the Minimum Period of Service; and

(b) any fees, charges, or costs paid by BT to a supplier that cannot be recovered from the supplier.

6.5.10 Paragraphs 6.1.4 and 6.1.6 of the Schedule will not apply.

6.5.11 Paragraph 6.2.13 of the Schedule will not apply.

6.5.12 Paragraphs 6.3, 6.4 and 6.5 of the Schedule will not apply.

6.6 **Proactive Monitoring**

BT will monitor the performance of the Managed Embedded Security Controls Service against parameters that BT deems appropriate.

6.6.1 Managed Service Package 1

(a) BT will monitor the performance of the Managed Embedded Security Controls Service at intervals set by BT and, where possible, provide advance warning to you through the Managed Services Portal of impending issues that may affect the Managed Embedded Security Controls Service and that BT identifies as a result of the monitoring. BT may not identify all impending issues.

(b) You are responsible for resolving the issues that BT provides you advance warning of in Paragraph 6.6.1(a).

(c) BT will check that the Managed Embedded Security Controls Service is operating correctly by:

(i) polling the Security Appliance to check it is powered on and has network connectivity. If the Security Appliance is not powered on or does not have network connectivity, the SOC will investigate and either take appropriate action or recommend action that you require to take;

(ii) Security Appliance status test: BT will test at regular intervals at BT's discretion as follows:

i. Resource status: conduct one test per Resource per Security Appliance such as CPU and RAM;
ii. physical status: conduct one test per physical attribute per Security Appliance such as temperature, where applicable to the Security Appliance;
iii. compare test results against standard vendor thresholds and notify any variances to the SOC. The SOC will investigate and either take appropriate action or recommend action that you are required to take;

(iii) Managed Embedded Security Controls Services access monitoring: generate alerts in near real time for unauthorised access attempts; and

(iv) application update status: on UTM/IDS/URLF and other applications selected as part of the Managed Embedded Security Controls Service.

(d) You will ensure that you or third parties, as required, configure routing/permissions on platforms or the Managed Embedded Security Controls Service to allow BT to carry out the monitoring.

6.6.2 Managed Service Package 2

(a) Both of us will agree a process for BT to contact you when it identifies an issue that impacts the Managed Embedded Security Controls Service.

(b) In addition to the checks carried out by BT in accordance with Paragraph 6.6.1(c), BT will check that the Managed Embedded Security Controls Service is operating correctly by monitoring the applications under the Managed Embedded Security Controls Service against parameters set by BT.

6.6.3 Managed Service Package 3

(a) In addition to the checks carried out in Paragraphs 6.6.1(c) and 6.6.2(b), BT will check that the Managed Embedded Security Controls Service is operating correctly by:

(i) password management including checking age and complexity of passwords, along with checking password hashes against known leaked password hash databases; and

(ii) certificate expiry monitoring. You are responsible for providing BT with updated certificates.

Part B – Service Delivery and Management

7 BT's Obligations

7.1 **Commissioning of the Service**

Before the Service Start Date, BT will:

7.1.1 on the date that BT has completed the activities in Paragraph 5.2 of the Schedule, confirm to you the date that the initial setup is complete, that the Controlled Deployment Period has commenced and the Service Start Date.

7.2 **During Operation**

On and from the Service Start Date, BT:

7.2.1 will maintain and will use reasonable endeavours to provide uninterrupted access to all pre-agreed and authorised Customer Contacts to the Managed Service Portal but BT does not guarantee that the Managed Service Portal will be available at all times or will be fault free; and

7.2.2 may, in the event of a security breach affecting the Managed Embedded Security Controls Service, require you to change any or all of your passwords.

7.3 **The End of the Service**

On termination of the Managed Embedded Security Controls Service by either of us, BT will terminate your access to the Embedded Security Controls and cease to provide all other elements of the Managed Embedded Security Controls Service.

8 Your Obligations

8.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the Managed Embedded Security Controls Service, you will:

8.1.1 establish and maintain your own internal support processes and helpdesk for Users and be responsible for communication with Users;

8.1.2 ensure that your firewall configurations and network settings allow the traffic types necessary for BT to provide the Managed Embedded Security Controls Service, including:

(a) ensuring that external HTTP, HTTPS and FTP over HTTP requests (including all attachments, macros or executables) are set up to be directed through the Managed Embedded Security Controls Service by making and maintaining the configuration settings required to direct external traffic via the Managed Embedded Security Controls Service, with BT's assistance and support as reasonably required and you acknowledge that this external traffic is dependent on your technical infrastructure; and

(b) ensuring that internal HTTP, HTTPS and FTP over HTTP traffic (e.g. to the corporate intranet) is not directed via the Managed Embedded Security Controls Service;

8.1.3 ensure that you order the appropriate Managed Embedded Security Controls Service features for your requirements;

8.1.4 provide BT with the WAN/LAN IP Address to enable BT to manage the Embedded Security Controls;

8.1.5 manage, and provide BT with accurate details of your internal IP Address design;

8.1.6 modify your network routing to ensure appropriate traffic is directed to the Embedded Security Controls;

8.1.7 ensure that your network and all applications conform to relevant industry standards and provide written confirmation to BT upon reasonable request;

8.1.8 configure your devices to enable them to connect to the Managed Embedded Security Controls Service; and

8.1.9 ensure that your Internet traffic can be routed through the Managed Embedded Security Controls Service.

8.2 **Controlled Deployment**

8.2.1 You will carry out the Controlled Deployment within the Controlled Deployment Period.

8.2.2 In respect of Managed Service Package 2 and Managed Service Package 3, both of us will jointly carry out the Controlled Deployment. You will use reasonable endeavours to complete the Controlled Deployment as early into the Controlled Deployment Period as possible.

8.2.3 You will notify BT when you have completed the Controlled Deployment. If you do not provide BT with such Notice by the end of the Controlled Deployment Period, the Controlled Deployment will be deemed to have been completed by you.

8.2.4 BT will notify you of the date of completion of the Controlled Deployment.

8.2.5 You will submit any changes you require to the CSP as a result of the Controlled Deployment through the SSR process set out in the Schedule.

8.3 **During Operation**

On and from the Service Start Date, you will:

8.3.1 monitor and maintain any Customer Equipment connected to the Managed Embedded Security Controls Service or used in connection with the Managed Embedded Security Controls Service, unless otherwise agreed with BT;

8.3.2 ensure that any Customer Equipment that is connected to the Managed Embedded Security Controls Service or that you use, directly or indirectly, in relation to the Managed Embedded Security Controls Service is:

(a) adequately protected against viruses and other breaches of security;

(b) technically compatible with the Managed Embedded Security Controls Service and will not harm or damage BT Equipment, the BT Network, or any of BT's suppliers' or subcontractors' network or equipment; and

(c) approved and used in accordance with relevant instructions, standards and Applicable Law and any safety and security procedures applicable to the use of that Customer Equipment;

8.3.3 immediately disconnect any Customer Equipment, or advise BT to do so at your expense, where Customer Equipment:

(a) does not meet any relevant instructions, standards or Applicable Law; or

(b) contains or creates material that is in breach of the Acceptable Use Policy and you are contacted by BT about such material,

and redress the issues with the Customer Equipment prior to reconnection to the Managed Embedded Security Controls Service;

8.3.4 provide BT with Notice 14 days in advance of any changes to your network that may impact the working of the Managed Embedded Security Controls Service, and provide BT with all necessary details. If this information is not provided within this timeframe, BT will have no liability for a failure or delay in providing any necessary changes to the Managed Embedded Security Controls Service configuration;

8.3.5 ensure that your Internet traffic can be routed through the Managed Embedded Security Controls Service; and

8.3.6 change your IP Address when requested by BT in accordance with Paragraph 6.2.3.

8.4 **The End of the Service**

On termination of the Managed Embedded Security Controls Service by either of us, you will disconnect the IPSec tunnel on your customer networking equipment from BT's Embedded Security Controls, otherwise your Internet bound traffic may not work.

Part C – Service Levels

9 Service Levels

9.1 There are no specific Service Levels for this Managed Embedded Security Controls Service.

Part D – Defined Terms

10 Defined Terms

In addition to the defined terms in the General Terms and the Schedule, capitalised terms in this Annex will have the below meanings (and in the case of conflict between these defined terms and the defined terms in the General Terms and the Schedule, these defined terms will take precedence for the purposes of this Annex). BT has repeated some definitions in this Annex that are already defined in the General Terms and the Schedule. This is to make it easier for you to find the definitions when reading this Annex.

"**Business Hours**" means between the hours of 0800 and 1700 in a Business Day.

"**Cardholder Data**" means the unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

"**Controlled Deployment**" means the fine tuning of your CSP(s), conducted by you or in respect of Managed Service Package 2 or Managed Service Package 3 only both of us jointly.

"**Controlled Deployment Period**" means in respect of:

(a) Managed Service Package 1, 48 hours after receiving Notice from BT in accordance with Paragraph 7.1.1;

(b) Managed Service Package 2, up to 30 Business Days after receiving Notice from BT in accordance with Paragraph 7.1.1; and

(c) Managed Service Package 3, up to 30 Business Days after receiving Notice from BT in accordance with Paragraph 7.1.1.

"**Customer Equipment**" means any equipment including any Purchased Equipment and any software, other than BT Equipment, used by you in connection with the Managed Embedded Security Controls Service.

"**Customer Security Policy**" or "**CSP**" means your security policy containing the security rules, set and owned by you, that are applied to the Managed Embedded Security Controls Service and determine the operation of the Managed Embedded Security Controls Service.

"**Domain Name System**" or "**DNS**" is a hierarchical and decentralised naming system for computers, services, or other resources connected to the Internet or a private network.

"**Embedded Security Controls**" means a software based network security system that uses rules to control incoming and outgoing network traffic.

"**File Transfer Protocol**" or "**FTP**" means standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet.

"**File Transfer Protocol Secure**" or "**FTPS**" means the name used to encompass a number of ways in which FTP software can perform secure file transfers. Each involves the use of a security layer below the standard FTP protocol to encrypt data.

"**General Terms**" means the general terms to which this Schedule is attached or can be found at www.bt.com/terms, and that form part of the Contract.

"**Hyper-Text Transfer Protocol**" or "**HTTP**" means an application protocol for distributed, collaborative, hypermedia information systems.

"**Hyper-Text Transfer Protocol Secure**" or "**HTTPS**" means a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet.

"**Identity Awareness/User Groups"** means the Service Option as set out in Paragraph 3.8.

"**Incident**" means an unplanned interruption to, or a reduction in the quality of, the Managed Embedded Security Controls Service or particular element of the Managed Embedded Security Controls Service.

"**Internet Message Access Protocol Secure**" or "**IMAPS**" is a mail protocol used to receive emails from a remote server to a local email client.

"**IP Address**" means a unique number on the Internet of a network card or controller that identifies a device and is visible by all other devices on the Internet.

"**IPS**" means intrusion detection and prevention service.

"**IPSec**" means Internet Protocol security; it is a standards-based framework that provides layer 3 services for confidentiality, privacy, data integrity, authentication and replay prevention.

"**MAC address**" means media access control address, a unique identifier assigned to a network interface controller for use as a network address in communications within a network segment.

"**Managed Embedded Security Controls Service**" has the meaning given in Paragraph 1.

"**Post Office Protocol 3 Secure**" or "**POP3S**" is a standard mail protocol used to receive emails from a remote server to a local email client.

"**Resource**" means a physical resource such as CPU or RAM present on a Security Appliance utilised during the use of the Security Appliance and exhaustion of that Resource would cause an Incident in or degradation of the Managed Embedded Security Controls Service.

"**Schedule**" means the Managed Service Schedule to the General Terms.

"**Security Appliance**" means the BT Equipment or Purchased Equipment that BT manages on your behalf as part of the Managed Embedded Security Controls Service used to apply the CSP(s). The Security Appliance may be physical or virtual.

"**Security Operations Centre**" or "**SOC**" means the BT team responsible for the proactive monitoring of the Managed Embedded Security Controls Service in accordance with Paragraph 6.6.

"**Service Management Boundary**" has the meaning given in Paragraph 4.1.
"**Service Options**" has the meaning given in Paragraph 3.
"**Simple Mail Transfer Protocol**" or "**SMTP**" is a communication protocol for electronic mail transmission.
"**Simple Mail Transfer Protocol Secure**" or "**SMTPS**" is a method for securing the SMTP using transport layer security.
"**Site**" means a location at which the Managed Embedded Security Controls Service is provided.
"**SSL**" means secure sockets layer.
"**SSL Encrypted Traffic**" means encrypted traffic transferred via the following protocols that BT will support for SSL/TLS Inspection:

(a) HTTPS;
(b) SMTPS;
(c) POP3S;
(d) IMAPS; and
(e) FTPS.

"**SSL/TLS Inspection**" means the Service Option as set out in Paragraph 3.7.
"**Standard Service Components**" has the meaning given in Paragraph 2.
"**Threat Emulation Service**" means the Service Option as set out in Paragraph 3.6.
"**VPN**" means a virtual private network with the use of encryption to provide a communications network that appears private to your Users while being provided over network infrastructure that is shared with other customers. Unless otherwise agreed in writing, your communications over your VPN are restricted to those Sites belonging to your VPN.